

§ 1311.50

(2) The person with power of attorney has had his or her privileges revoked.

(b) A registrant must maintain a record that lists each person granted power of attorney to sign controlled substances orders.

§ 1311.50 Requirements for recipients of digitally signed orders.

(a) The recipient of a digitally signed order must do the following before filling the order:

(1) Verify the integrity of the signature and the order by having the system validate the order.

(2) Verify that the certificate holder's CSOS digital certificate has not expired by checking the expiration date against the date the order was signed.

(3) Check the validity of the certificate holder's certificate by checking the Certificate Revocation List.

(4) Check the certificate extension data to determine whether the sender has the authority to order the controlled substance.

(b) A recipient may cache Certificate Revocation Lists for use until they expire.

§ 1311.55 Requirements for systems used to process digitally signed orders.

(a) A CSOS certificate holder and recipient of an electronic order may use any system to write, track, or maintain orders provided that the system has been enabled to process digitally signed documents and that it meets the requirements of paragraph (b) or (c) of this section.

(b) A system used to digitally sign Schedule I or II orders must meet the following requirements:

(1) The cryptographic module must be FIPS 140-2, Level 1 validated, as incorporated by reference in § 1311.08.

(2) The digital signature system and hash function must be compliant with FIPS 186-2 and FIPS 180-2, as incorporated by reference in § 1311.08.

(3) The private key must be stored on a FIPS 140-2 Level 1 validated cryptographic module using a FIPS-approved encryption algorithm, as incorporated by reference in § 1311.08.

(4) The system must use either a user identification and password combina-

21 CFR Ch. II (4-1-05 Edition)

tion or biometric authentication to access the private key. Activation data must not be displayed as they are entered.

(5) The system must set a 10-minute inactivity time period after which the certificate holder must reauthenticate the password to access the private key.

(6) For software implementations, when the signing module is deactivated, the system must clear the plain text private key from the system memory to prevent the unauthorized access to, or use of, the private key.

(7) The system must be able to digitally sign and transmit an order.

(8) The system must have a time system that is within five minutes of the official National Institute of Standards and Technology time source.

(9) The system must archive the digitally signed orders and any other records required in part 1305 of this chapter, including any linked data.

(10) The system must create an order that includes all data fields listed under § 1305.21(b) of this chapter.

(c) A system used to receive, verify, and create linked records for orders signed with a CSOS digital certificate must meet the following requirements:

(1) The cryptographic module must be FIPS 140-2, Level 1 validated, as incorporated by reference in § 1311.08.

(2) The digital signature system and hash function must be compliant with FIPS 186-2 and FIPS 180-2, as incorporated by reference in § 1311.08.

(3) The system must determine that an order has not been altered during transmission. The system must invalidate any order that has been altered.

(4) The system must validate the digital signature using the signer's public key. The system must invalidate any order in which the digital signature cannot be validated.

(5) The system must validate that the DEA registration number contained in the body of the order corresponds to the registration number associated with the specific certificate by separately generating the hash value of the registration number and certificate subject distinguished name serial number and comparing that hash value to the hash value contained in the certificate extension for the DEA registration number. If the hash values are not

equal the system must invalidate the order.

(6) The system must check the Certificate Revocation List automatically and invalidate any order with a certificate listed on the Certificate Revocation List.

(7) The system must check the validity of the certificate and the Certification Authority certificate and invalidate any order that fails these validity checks.

(8) The system must have a time system that is within five minutes of the official National Institute of Standards and Technology time source.

(9) The system must check the substances ordered against the schedules that the registrant is allowed to order and invalidate any order that includes substances the registrant is not allowed to order.

(10) The system must ensure that an invalid finding cannot be bypassed or ignored and the order filled.

(11) The system must archive the order and associate with it the digital certificate received with the order.

(12) If a registrant sends reports on orders to DEA, the system must create a report in the format DEA specifies, as provided in §1305.29 of this chapter.

(d) For systems used to process CSOS orders, the system developer or vendor must have an initial independent third-party audit of the system and an additional independent third-party audit whenever the signing or verifying functionality is changed to determine whether it correctly performs the functions listed under paragraphs (b) and (c) of this section. The system developer must retain the most recent audit results and retain the results of any other audits of the software completed within the previous two years.

§ 1311.60 Recordkeeping.

(a) A supplier and purchaser must maintain records of CSOS electronic orders and any linked records for two years. Records may be maintained electronically. Records regarding controlled substances that are maintained electronically must be readily retrievable from all other records.

(b) Electronic records must be easily readable or easily rendered into a format that a person can read. They must

be made available to the Administration upon request.

(c) CSOS certificate holders must maintain a copy of the subscriber agreement that the Certification Authority provides for the life of the certificate.

PART 1312—IMPORTATION AND EXPORTATION OF CONTROLLED SUBSTANCES

Sec.

- 1312.01 Scope of part 1312.
1312.02 Definitions.

IMPORTATION OF CONTROLLED SUBSTANCES

- 1312.11 Requirement of authorization to import.
1312.12 Application for import permit.
1312.13 Issuance of import permit.
1312.14 Distribution of copies of import permit.
1312.15 Shipments in greater or less amount than authorized.
1312.16 Cancellation of permit; expiration date.
1312.17 Special report from importers.
1312.18 Contents of import declaration.
1312.19 Distribution of import declaration.

EXPORTATION OF CONTROLLED SUBSTANCES

- 1312.21 Requirement of authorization to export.
1312.22 Application for export permit.
1312.23 Issuance of export permit.
1312.24 Distribution of copies of export permit.
1312.25 Expiration date.
1312.26 Records required of exporter.
1312.27 Contents of special controlled substances invoice.
1312.28 Distribution of special controlled substances invoice.
1312.29 Domestic release prohibited.
1312.30 Schedule III, IV, and V non-narcotic controlled substances requiring an import and export permit.

TRANSSHIPMENT AND IN-TRANSIT SHIPMENT OF CONTROLLED SUBSTANCES

- 1312.31 Schedule I: Application for prior written approval.
1312.32 Schedules II, III, IV: Advance notice.

HEARINGS

- 1312.41 Hearings generally.
1312.42 Purpose of hearing.
1312.43 Waiver or modification of rules.
1312.44 Request for hearing or appearance; waiver.
1312.45 Burden of proof.
1312.46 Time and place of hearing.
1312.47 Final order.